Mobile Computing Decision Framework

May 23, 2013

Table of Contents

Executive Summary

Organizations considering the deployment of mobile devices will need to make a number of important decisions. These decisions often include an examination of the following:

- How mobile technology will support the organization's mission;
- What platforms will be supported;
- What technologies will be used to support mobile devices; and
- Who will manage the solution.

The Mobile Computing Decision Framework (MCDF) provides a holistic decision-making process that assists organizations in determining which mobile solution, if any, will support their organizational missions. While completing the four stages of this framework, an organization will:

- Understand the appropriateness of mobile solutions in the light of its mission and goals;
- Reach a suitable balance between capabilities, security, and economics in order to identify risks;
- Assign each risk to one of the seven risk categories[1] to determine residual risks and how the organization will address them; and
- Be able to evaluate and compare vendor solutions with respect to the organization's needs and select the best-fit solution.

The MCDF process can be customized by each organization to meet its unique needs and processes and to work within established Federal guidance and risk management frameworks.

[1] The seven risk categories are those developed by the Mobile Technology Tiger Team formed by the Federal CIO Council.

Introduction

The rate of mobile technology innovation in today's market is increasing constantly. The accelerating pace of development and the proliferation of new products present opportunities for an advantageous course of innovation in the ways an enterprise communicates and delivers services. But at the same time, the mobile market's momentum is driving Departments and Agencies (D/A) to make quicker decisions in both selection and implementation. To ensure that their decisions make the best possible contribution to mission fulfillment, D/As need the tools of a uniform decision framework for mobile computing.

A Mobile Computing Decision Framework (MCDF) was proposed and prototyped in December 2012[2] as a tool for Chief Information Officers (CIOs) considering investment in mobile solutions. The prototype MCDF (Figure 1: The Mobile Computing Decision Framework) delivered at that time was intended to:

- Provide a common framework and uniform approach for selecting mobile solutions;
- Identify mission requirements and use cases for mobile computing;
- Build understanding of tradeoff considerations and organizational risks;
- Support the selection of information technology (IT) assets for mobile computing;
- Measure current mobile computing investments; and
- Support justification of mobile computing investments.

The MCDF has evolved to support the vision of the Digital Government Strategy[3] and to provide a holistic approach to considerations for decisions that support a secure mobile computing solution.

[2] The prototype MCDF was a result of Digital Government Strategy Milestone 10.2, and was made a part of Milestone 9.1. It was prepared by the Mobile Technology Tiger Team (MTTT) with direction from the Information Security and Identity Management Committee (ISIMC) and the Federal CIO Council.
[3] See http://www.whitehouse.gov/digitalgov.

Framework Overview

The MCDF is a holistic decision-making process that helps organizations select a mobile computing solution. There are four distinct stages of the MCDF:

- Mission Requirements;
- Decision Balancing;
- Risk-Based Tailoring; and
- Results.

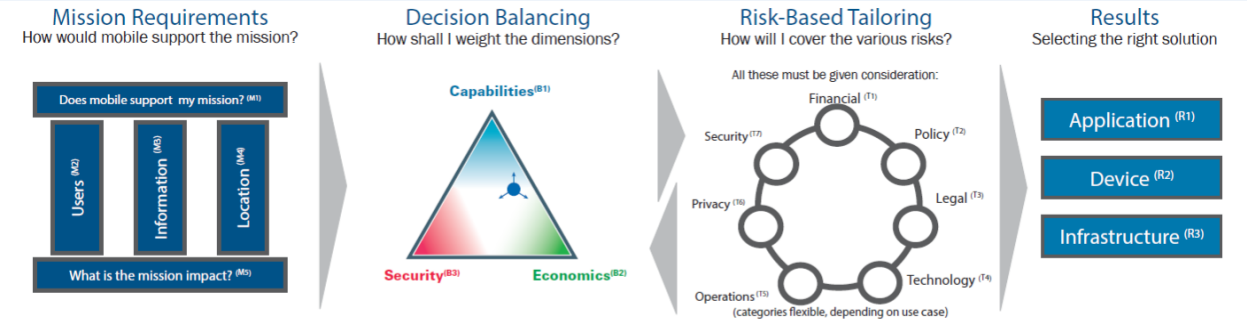

Figure 1: The Mobile Computing Decision Framework

Each of these stages provides insight into both the overall usability of a given mobile solution for an organization and the risks and tradeoffs associated with its implementation. Organizations must apply this framework on a per-mission basis because each mission may have a unique set of requirements and acceptable risks.

The ***Mission Requirements*** stage helps organizations to determine whether the addition of a mobile solution is right for them. Completing the Mission Requirements stage helps the organization build a use case for mobile computing by establishing who needs access to what, where they need access to it, and why access is required. An organization must understand the needs of the personnel (both internal and external) who support the mission, the information they must access, and the physical location and mission criticality under which the information must be accessed.

An organization reaches the ***Decision Balancing*** stage when it has established a sufficient need to implement a mobile solution for a given mission. Implementing the chosen solution, however, entails tradeoffs determined by the mission requirements; these relate to the following three major considerations:

- Capabilities – what an authorized user must be able to do with the information;
- Security – how secure the information must be; and
- Economics – how much the organization can afford to spend to obtain the desired security and capabilities, and how can it leverage existing capabilities.

Balancing these three considerations helps to define the significance of a mobile solution's risks and the extent of risk mitigation measures.

The bulk of an organization's MCDF work is done in the ***Risk-Based Tailoring*** stage. Based on the starting point chosen in the Decision Balancing stage, the organization can use risk frameworks, such as National Institute of Standards and Technology (NIST) Special Publications (SP) 800-37[4] and 800-39,[5] to identify risks in seven key categories, which are represented in the diagram shown in Figure 5. If the risks are considered too great, the organization can return to the Decision Balancing stage to modify the balance of capabilities, security, and economics. After choosing a new starting point, the organization returns to the Risk-Based Tailoring stage to determine if the risk across the seven categories is more acceptable. If not, further iterations are required.

Finally, the ***Results*** stage translates the acceptable risks from the Risk-Based Tailoring stage, the balanced considerations from the Decision Balancing stage, and the requirements from the Mission Requirements stage into actionable requirements for the specification of a mobile solution that will fit the mission's needs. Organizations can use the MCDF to obtain a high-level understanding of the relationships among its applications, devices, infrastructure, and mobile solution.[6]

Mobile Computing Decision Framework

Mission Requirements

The first step in determining whether an organization would benefit from the addition of a mobile solution is to develop an understanding of which organizational missions are candidates for a mobile solution. Then, for each candidate mission, the organization must determine *who* needs mobile access, to *what* data, *why*, and *where*.

Every individual assigned to an organizational mission may not need a mobile device. Determine which user groups make up the mobile workforce for each candidate mission. User groups may be public, partner, state, local, tribal, or territorial. They may be Federal employees. They may be personnel who use National Security Systems.[7] To determine if a user requires access to a mobile solution, consider the following questions:

- Does the user's mission role require travel?
- Does the user work in locations where a laptop or desktop computer is impractical?
- Does the user have physical limitations that make a mobile solution more practical to use?

[4] NIST Special Publication SP800-37 "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach."
[5] NIST Special Publication SP800-39 "Managing Information Security Risk: Organization, Mission, and Information System View."
[6] The MCDF aligns with NSA Enduring Security Framework efforts.
[7] Please see Mobile Security Reference Architecture Section 3.1 for details.

- Does the user require functionality that is not supported by or that is impractical on a conventional desktop or laptop?
- Does the potential user have on-call duties?
- Is the user prevented from participating in existing workflows with individuals from relevant partner organizations who already have mobile functionality?
- With what policies must the potential solution comply?
- What regulatory requirements will influence selection of a solution?

This list of questions is not exhaustive, but it can serve as a starting point for a complete characterization of the potential mobile device users in an organization.

After identifying a set of potential users for each mission, determine the types of data that these potential users must access to support the mission. Not all mission data needs to be, or should be, remotely accessible. Develop an understanding of how mission data is stored. Determine whether it is possible to limit the types of data exposed to a mobile solution. Key questions to answer at this point are the following:

- To what data must a potential mobile solution have access?
- Are there restrictions on the data (e.g., Sensitive But Unclassified (SBU), Personally Identifiable Information (PII), etc.)?
- Where would the data be stored—on enterprise systems, on the mobile devices, on third party providers' systems, or on some combination of these?
- How much data would be transferred over a mobile solution?
- How does the agency provide access to its users?
- How is identity assurance achieved?

Construct a list of potential data sources that could be exposed to a mobile solution. The organization will use this list extensively in the MCDF's Decision Balancing and Risk-Based Tailoring stages. To identify data type and potential data sources, organizations may find it helpful to consult the Certification and Accreditation (C&A) or Assessment & Authorization (A&A) packages of existing systems that will be used to support the mobile solution.

Finally, for each group of potential users, identify a set of remote location types where the mobile user will support the mission. Examples include partner organization offices, construction work sites, law enforcement or military field operation areas, field inspection sites, disaster and emergency response areas, non-organizational meeting facilities, and homes. Each identified location type has its own set of characteristics to consider during the Decision Balancing and Risk-Based Tailoring stages. Also identify and list locations not appropriate for mobile access to mission data, and define any known limitations on wireless connectivity at the user location.

At this point, the organization's leadership should review all of the information collected on mobile solutions for each mission and evaluate it in light of the organization's goals. If any portion of the information collected for a mission presents a red flag, or conflicts with the organization's goals, then

leadership should reconsider implementing a mobile solution for that mission component. Once all red flags have been addressed, the organization can continue to the next stage.

Decision Balancing

The solution ultimately implemented will be subject to constraints imposed by security and economic concerns; these must be balanced against the capabilities in a process known as Decision Balancing. Figure 2: The Decision Balancing Triangle, illustrates how giving more weight to one of the factors constrains the others, moving the Decision Balance Point. The three decision balancing factors are defined as follows:

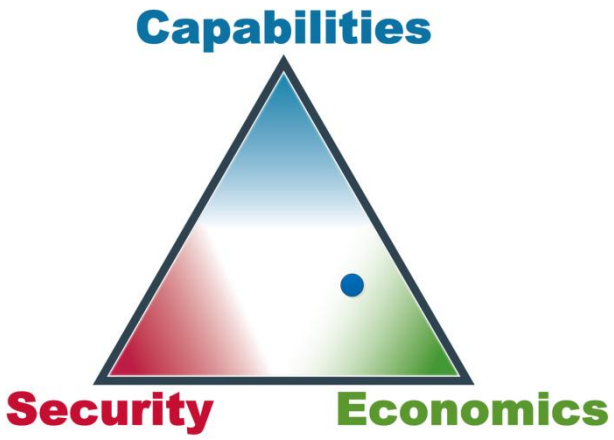

Figure 2: The Decision Balancing Triangle

Capabilities

The closer a point is to the capabilities vertex, the more important the ability to support a wide range of applications and uses becomes. In general, every mobile application that a mission uses requires increased device capability.

Security

The closer a point is to the security vertex, the more important security is to the mission. Some missions, such as those dealing purely with publicly available information, do not require strong security, but information must be appropriately tagged and labeled for release to the public. Other missions, such as those that use Sensitive but Unclassified (SBU) information or Controlled Unclassified Information (CUI) have a strong need for security.

Economics

The closer a point is to the economics vertex, the more important availability, cost, and user familiarity become. Economics includes not only the overall cost of a solution, including training and support, but also the availability of commoditized components.

The Decision Balance Point is represented by the blue dot in Figure 2. The closer the Decision Balance Point is to a particular factor's vertex, the more important balancing has made that factor.

The relationship between security and capability is a constant in today's markets. As the capability of a mobile solution increases, so too does its complexity. As complexity increases, the number of potential vulnerabilities increases, putting greater demands on system security. An organization must determine the optimal set of capabilities required of the solution, because excess capabilities may compromise security.

There is also a general relationship between security and economics. In general, more commonly available components are cheaper and easier to deploy in a large organization, but cheaper solutions are likely to have fewer capabilities. Additional capabilities may incur additional costs for licensing, support, and training.

More secure solutions are likely to require more support and user training, but are often less readily available in the marketplace. Less secure solutions are more readily available in the marketplace and achieve broader consumer adoption than more secure solutions because user familiarity with a solution reduces the cost of training and support.

Balancing economics and capability is fairly straight forward. Increasing capability will almost surely increase cost. Each capability added to the feature set reduces the number of mobile devices that can meet the need and is likely to impact overall security. In addition, some developers do not offer their applications for a given operating system due to the challenges of supporting the wide range of hardware that uses that operating system; as a result, platform availability decreases, and cost tends to increase.

Usability of a mobile solution is paramount, but may be adversely affected if users think that security controls hamper their ability to perform their duties or mission. Users may look for ways to circumvent security, or they may not use the solution at all. Users also avoid solutions that contain overly complex applications, as well as solutions that do not fit a known business model or workflow. Many providers of commercial mobile solutions conduct usability studies for their products. A review of these studies will help determine which solutions best fit the mission environment.

The first step in determining the Decision Balance Point using the Decision Balancing triangle is to review the mission requirements gathered in the mission requirements stage of the MCDF. Assign a priority to each mission requirement based on its overall mission impact. Then, given economic constraints, identify which mission requirements, if any, could be acceptably cut. Create a list of data sources used by the mission requirements and assign a security value to each source. The security value should reflect how important the confidentiality, integrity, and availability of the data source is to the organization.

To determine mission requirement priority and security value, the following basic questions about the mission should be answered:[8]

- What mobile capabilities do users require to perform the mission?
- What is the sensitivity of the data that will be accessible by the mobile solution?
- What are the potential consequences to the mission of a data spillage?
- Are there limits to the long-term costs associated with the mobile solution?
- Are there additional technologies that will need to be licensed and implemented to support the mobile solution?

This process should yield two tables, as shown in Figure 3: Ordering Mission Requirements.

Mission Requirements		
	Priority	Total Security Value
Requirement 1	100	135
Requirement 2	95	25
Requirement 3	70	45
Requirement 4	60	90
Requirement 5	33	15
Requirement 6	25	150

Missions Ordered by Priority

Mission Requirements		
	Priority	Total Security Value
Requirement 6	25	150
Requirement 1	100	135
Requirement 4	60	90
Requirement 3	70	45
Requirement 2	95	25
Requirement 5	33	15

Missions Ordered by Security Value

Figure 3: Ordering Mission Requirements

The red line in the priority-ordered table shows the cut point based on economic constraints. The red line in the security-ordered table shows the cut point based on a chosen security threshold value.

To define the Decision Balance Point, divide the number of requirements below the red line in the priority-ordered table by the total number of requirements in the table. The resulting fraction defines a point along the capability-economics side of the triangle (previously shown in Figure 3), as measured from the economics vertex.

[8] These questions are not exhaustive, but a starting point to the Decision Balancing discussion. The Digital Government Strategy and NIST Special Publications are resources for amplifying discussion:

- The Digital Government Strategy
- NIST SP 800-164: Draft Guidelines on Hardware-Rooted Security in Mobile Devices
- NIST SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing
- NIST SP 800-137: Information Security Continuous Monitoring for Federal Information Systems and Organizations
- NIST SP 800-124: Draft Guidelines for Managing and Securing Mobile Devices in the Enterprise

Next, sum the mission security values above the red line in the priority table, and divide by the total of the security values of all the mission requirements in the table. This fraction will define a point along the Security-Economics side, as measured from the security vertex.

The third step is to decide on a threshold that will separate "low security" from "high security." This can be an average of all security values, or it can be one or two standard deviations above or below the average. The red line in the security-ordered table shows the cut point based on a chosen security threshold. Divide the number of mission requirements above the threshold by the total number of mission requirements. This fraction represents a point along the Capabilities-Security side of the triangle as measured from the capabilities vertex.

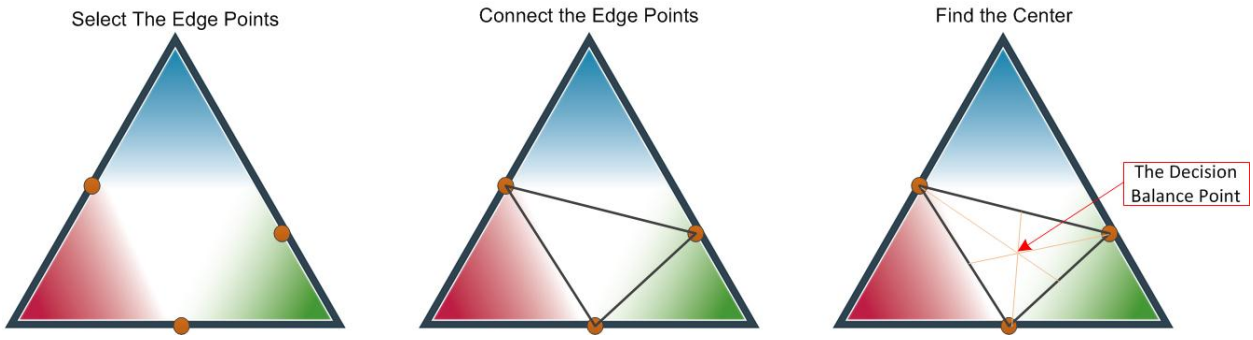

Figure 4: Locating the Decision Balance Point

Once points have been calculated for all three sides, find the Decision Balance Point as shown in Figure 4: Locating the Decision Balance Point. Connecting the three edge points together in an internal triangle creates the center of the internal triangle that is the Decision Balance Point.

After determining a Decision Balance Point within the Decision Balancing Triangle, the organization can use it in discussing Risk-Based Tailoring, considering the relative importance of capabilities, security, and economics to the mission. The interplay between Decision Balancing and Risk-Based Tailoring is iterative; if the results of the Risk-Based Tailoring process are not entirely acceptable, start at a new point in the Decision Balancing stage and repeat the process until an acceptable outcome is achieved.

Risk-Based Tailoring

The seven categories of risk illustrated, in Figure 5: The Risk Categories, should be assessed when choosing a mobile computing solution. The Mobile Technology Tiger Team identified these as the risks of greatest concern to the Federal Government. They are flexible and somewhat subject to interpretation based on an organization's use cases, risk concerns, and risk tolerance.

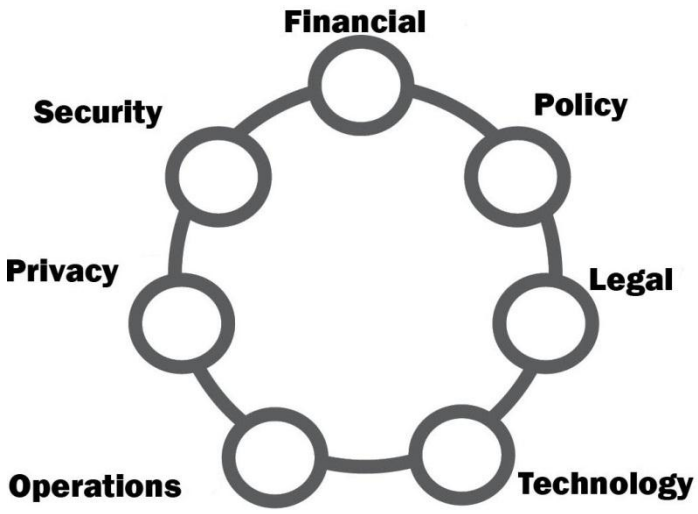

Figure 5: The Risk Categories

To begin assessing the risks associated with a mobile solution, first consider the relative importance of security, capabilities, and economics, as determined in the Decision Balancing stage of the MCDF. Using those factors, refer to NIST SP 800-39, particularly Section 3.1, "Framing Risk," and Section 3.2, "Assessing Risk," to help identify key risks in each of the seven categories.

NIST SP 800-39 provides "guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of federal information systems."[9]

The Appendix A contains a mapping of each area of risk to its relevant NIST SP 800-53 control families; this mapping may be useful to organizations in defining their risks in each of the seven risk categories.

Financial Risks

Financial risk considerations include costs related to supply chain risk, incident management, deployment, training, vendor support, solution operations, software and hardware maintenance, and platform switchover, as well as the costs associated not only with remediation following an incident, but also costs of public relations efforts needed to restore the organization's reputation after a security incident. All of these risks contribute to the importance of the economics factor in the Decision Balancing stage. Ask the following basic questions when evaluating financial risks:

[9] NIST, *Managing Information Security Risk (NIST SP 800-39).* http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf (2011).

- Is there positive value in delaying the mobile computing rollout in anticipation of a government-wide contract vehicle for devices and data plans?[10]
- What supply chain and acquisition issues must be addressed?
- What are the risks of "vendor lock-in" and switching platforms, and what are the costs of avoiding them?
- How quickly does mobile technology advance, and does the organization need to keep up with leading-edge trends?
- Does the organization already provide mission services and data using a platform that is incompatible with mobile solutions? If so, what are the risks and costs of migration to a new mobile supporting platform?
- What are the long-term financial costs and risks of modifying or replacing the mobile infrastructure (devices, service platforms, Mobile Device Management (MDM), wireless network infrastructure, etc.)?
- In the event that critical information is stored only on a mobile device, what are the costs associated with data recovery for a lost, stolen, or damaged device?
- In the event of information spillage, what are the associated costs of mitigation and remediation?

Deployment and training also might incur cost overruns or additional expenses related to long-term vendor support for the solution. Issues arising during the operations and maintenance phase of a solution not anticipated during implementation and deployment may further increase costs. In general, the more importance the capabilities consideration was given in the Decision Balancing stage, the greater the potential financial risks.

Policy Risks

Policy considerations include determining what modifications to existing policies, and what new policies the organization will need in order to support mobile computing. Where existing policies impact mobile computing, the organization will need to establish timelines for policy modification or replacement. Given the evolving nature of mobile computing, the organization must consider the need for parallel policy evolution and approval; it may be necessary to seek waivers or exceptions pending publication of revised policies.

Ask the following basic questions when evaluating policy risks:

- To what extent will the organization require control over its mobile devices?
- Who owns the information residing on the devices?
- How does the organization want to define what organizational information is allowed to be stored on the device? How would the policy be enforced?

[10] https://cio.gov/wp-content/uploads/downloads/2012/12/Government_Mobile_Technology_Barriers_Opportunities_and_Gaps.pdf.

- What types of personalization are mobile device users allowed to perform?
- Does existing policy cover future technical capability?

When new policies are written, or existing policy elements modified, the rapidity of innovation in the marketplace should be considered so that continual modification of policy elements will be minimized.

Placing high importance on capabilities may incur additional policy risks. The organization can use policy to supplement or replace technical controls, but that option carries its own risks. If an organization relies on policy to moderate user behavior, inadvertent or malicious user actions might not be detected until damage is sustained.

When supplementing technical controls with policy, an organization must also consider balancing policy with usability. Policies and technical controls that are too strict or complex might deter the use of mobile computing. All policies should carry a deterrent that the organization can apply easily and fairly. Users seeking expedience will often ignore policies that have no consequences.

In general, the more distant the Decision Balance Point is from the security vertex in the Decision Balancing Triangle, the more important policy and an understanding of policy risks become.

Legal Risks

The capabilities and security vertices of the Decision Balancing Triangle have associated legal risks. Users must be informed that the organization has the right to monitor their activities, and that they can have no expectation of privacy. The organization must also consider the e-discovery, data-retention, and data disposition rules that apply to mobile devices because these rules may differ from the rules used on current enterprise systems.

Ask the following basic questions when evaluating legal risks:

- What Rules of Behavior (ROB) and monitoring policies will be necessary to inform users of their expected behavior and to serve as a basis for legal or employment actions against violators?
- What type of use agreement will be necessary to inform users of the remote wipe policies (including what data will be wiped)?
- What documentation of consent may be needed or required before the organization can monitor or search an employee's device?
- What capabilities that satisfy Freedom of Information Act (FOIA) and other legal requirements does the solution have for support of e-discovery and data-retention?
- Do the solution's communications providers have their own discovery, data retention, and data breach notification policies for Short Message Service (SMS) messages, call history, voicemail, etc.?
- Does the solution meet the requirements of applicable Federal laws, Executive Orders, directives, policies, guidance, and regulations?
- What are the liability implications of a breach or information spillage?
- What security related obligations must be included in contracts and Service Level Agreements (SLA) with communications providers?

Unlike the other risk categories, legal risks are not affected by the choice of a Decision Balance Point. Legal risks such as those surrounding the use of PII derive from existing and future legislation, legal precedents set by judicial rulings, and organizational policy. It is prudent to consult the organization's legal counsel during all stages of the MCDF to assist in the minimization of legal risks.

Technical Risks

Technical risks are introduced when new capabilities are added to a solution and when new security measures are implemented. New capabilities provide greater functionality, but they also introduce the risk of exploitation by malicious actors. In general, the more complex a new capability is, the greater the new functionality's potential to add risk. New security features add complexity to a solution. Users may find the increased complexity cumbersome and attempt to circumvent the new features, increasing risk.

Ask the following basic questions when evaluating technical risks:

- What current organizational infrastructure can be leveraged for mobile computing?
- What new infrastructure elements will be needed?
- What applications and services will need to be developed and supported for the mobile solution?
- What are the risks of adopting new and immature technology versus old technology that may soon reach the end of its life?
- Can the mobile computing solution enforce a network boundary to identify, isolate, and protect the mobile devices?
- What types of device security (device encryption, passcodes, etc.) are required to protect the information on the device? How will users utilize these features?
- What are the ergonomic and environmental considerations for the devices?

One method of reducing the risk added to a solution is to take advantage of existing organizational infrastructure such as virtualization, content management, or filtering solutions. These infrastructure elements are already well understood by the organization's personnel, and the risks associated with them have already been mitigated to an acceptable level. In addition, vendors of virtualization capabilities often have tailor-made solutions available for accessing capabilities from mobile solutions that reduce the risk associated with getting multiple vendors' technologies to work together seamlessly.

An organization should also consider the long-term stability required by the solution. The mobile computing market is very fluid, and solutions come and go quickly. When determining which mobile devices, operating system(s), and software to support, consider the impact of choosing a technology that could become obsolete or cease to be available. Also, be aware that certain software might be available only on certain platforms and, consequently, may be more or less mature depending on the specific platform.

Operational Risks

Organizations need to consider how to implement the mobile technology in their organization and who will manage the service. These considerations are associated with the capabilities vertex of the Decision

Balancing Triangle because adding capabilities increases operational risks. Ask the following basic questions when evaluating operational risks:

- How will mobile computing affect contingency planning and mission assurance?
- How will mobile computing affect incident response policies and procedures?
- What training, if any, will users require?
- What expertise and resources are needed to provision, configure, and manage the mobile infrastructure, devices, and applications?
- Will IT staff need to be augmented or trained?
- If the organization will need to hire additional staff to support the mobile solution, are people with the necessary skills readily available? If not, how long will it take time to hire them?

Mobile solutions require a contract with trusted business partners, at a minimum with a cellular service provider. Depending on the solution, the organization may also select a separate service provider to manage mobile devices, applications, services, and associated security policies. The organization might need to train, hire, or reposition personnel sufficiently to develop, manage, and support the mobile computing assets and ensure operational redundancy.

Privacy Risks

The organization must consider privacy implications before selecting and deploying a mobile solution. Privacy considerations are associated with the security vertex of the Decision Balancing Triangle because privacy risks are reduced by a strict security posture. Ask the following basic questions when evaluating privacy risks:

- What are the privacy implications of tracking mobile devices?
- How do privacy laws differ by state and country?
- How will the mobile solution provide privacy and content notices to users prior to using the systems?
- What privacy risks and data exfiltration risks are associated with solutions that have peripheral functionality (camera, video, geo-location, etc.)?
- How will the organization address privacy and safety risks of using location information?
- How will the solution protect personal data in the case of personal use of government-furnished equipment devices?
- What data do mobile applications collect and how is that data used? Can the mobile application leak sensitive data to a third party?
- Is there a risk of a mobile device exposing PII belonging to other users of the same mobile system?
- Will personal use of mobile devices be allowed? How will information about those uses be treated?

Policies and procedures will be required for identifying, handling, and accessing personal data on personally owned devices. Policies and procedures should also address who can access information about the location of a mobile user, when they can access it (e.g., business hours versus personal time),

and how they can use it (e.g., only for permitted applications). An individual's location can be sensitive information, and only a limited number of people with a need to know should have access to it. The organization will also need to establish policies regarding personal use of government furnished equipment. The organization will need to conduct a privacy impact assessment (PIA) to determine the full level of risk involved.

Security Risks

The importance of security considerations increases as the decision balance point nears the security vertex. Ask the following basic questions when evaluating security risks:

- Does the mobile solution support FIPS-validated cryptographic modules for authentication and encryption, as required by law?
- How does the rapid refresh cycle of mobile devices affect security configurations?
- Does the solution allow for destruction of enterprise data in the event of a loss or compromise?
- Can the mobile solution enforce the relevant NIST 800-53 control families as defined in the mobile security baseline?
- Does the solution include the ability to prevent malicious software from executing on the device?
- Does the mobile solution support requirements for two-factor authentication?
- Is data that will be exposed to the mobile solution appropriately tagged and labeled for release?

Security considerations include determining if the current technology affords necessary security controls such as encryption, authentication, and configuration verification. The solution should permit the agency to specify:

- Who are the users, and how are they authenticated?
- What activities users can and do perform via configuration management and auditing?
- What devices can connect to the enterprise, and how they can connect (particular access points, VPN, etc.)?

Consider the risks of enabling users to download untrusted applications that may compromise the device or enterprise data if said data are not adequately sandboxed. Ensure that the level of security controls and protection is commensurate with the data that users access with the device. In addition, consider the enterprise systems to which the mobile solution will connect and what additional security risks it will introduce to those systems.

Risk Methodologies

Before deploying a mobile solution, the organization should follow its risk management strategy and methodology and should review risk management guidance that may assist in determining the best solution for the enterprise:

- NIST SP800-64 "Security Considerations in the Systems Development Life Cycle" discusses incorporating security into the various stages of a system's life cycle, including initiation,

development and acquisition, implementation and assessment, operations and maintenance, and disposal.[11]

- NIST SP800-37 Revision 1 "Guide for Applying the Risk Management Framework to Federal Information Systems" provides guidance for conducting activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring.[12]
- NIST SP800-124 (Draft) "Guidelines for Managing and Securing Mobile Devices in the Enterprise" provides "… recommendations for selecting, implementing, and using centralized management technologies, and it explains the security concerns inherent in mobile device use and provides recommendations for securing mobile devices throughout their life cycles."[13]
- NSA's Mobility Capability Package "…describes the Enterprise Mobility Architecture, a layered security approach for using commercial devices and networks to securely connect mobile users to the Government enterprise."[14]

After completing the Risk-Based Tailoring stage, the organization should have a set of guidelines for the purchase of a mobile solution and a set of residual risks that need to be addressed. The organization should use its existing risk management guidelines to help determine how well a given risk area has been covered. If the risks of implementing a mobile solution are unacceptable to the organization, it may revisit the Decision Balancing stage to choose a new starting point and perform further iterations until a more acceptable set of risks and guidelines are determined.

Results

The Decision Balancing and Risk-Based Tailoring stages help an organization produce guidelines and considerations for how best to position a mobile computing solution in the enterprise. Using those guidelines and considerations, the organization should determine what aspects of infrastructure, mobile devices, and applications will best promote mission accomplishment. If the guidelines produced during the Decision Balancing and Risk-Based Tailoring stages are too vague, too restrictive, or simply not in line with the needs and desires of the organization, then the organization can revisit the Decision Balancing stage, select a new starting point, and reiterate the process until an acceptable outcome is achieved.

Once an acceptable set of criteria has been produced, the organization will follow its engineering life cycle process to develop an engineering requirements package for a mobile computing solution. The organization can then use the requirements package as a basis for discussion with vendors. Each vendor will provide a proposed set of specific implementations of mobile technologies, infrastructure, and support packages that should address the mission requirements defined in the engineering package. There are a number of things to consider when evaluating vendor solutions, which fall into three broad

[11] http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf.
[12] http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.
[13] http://csrc.nist.gov/publications/drafts/800-124r1/draft_sp800-124-rev1.pdf.
[14] http://www.nsa.gov/ia/_files/Mobility_Capability_Pkg_Vers_2_1.pdf.

categories discussed below. The proposed solutions should be compared with each other and with the requirements package.

Infrastructure

- What type of infrastructure is needed to support the mobile solution? Can the organization augment and use the existing infrastructure?
- Is the necessary infrastructure commodity based or highly specialized?
- Does the solution require the use of an infrastructure (such as third party cloud services) that is not controlled by the organization?
- What type of vendor support is required for the solution? Is there a constant presence required or is support provided on an "as needed" basis?
- Are there regulations or policies that govern the types and configurations of infrastructure that can be used, such as the Trusted Internet Connection (TIC) initiative?
- Where will data be stored, which applications can access it, and how will it be transported?
- Is data stored by the solution protected (cryptographically, etc.) both at rest and during transport?
- How will the physical devices be managed and secured?
- Does the solution require extensive knowledge of technologies not previously used by the organization?
- Will the infrastructure support a single mobile device platform or multiple platforms?
- Is the infrastructure scalable to provide support to additional missions in the future? Can scaling be accomplished without additional vendor support?

Mobile Devices

- Which platforms will be supported?
- How will policies and procedures be enforced on the mobile devices?
- Will the organization support personal (enabled or dual persona) devices?
- Who is responsible for lost, stolen, or damaged devices?
- Who will be eligible to participate in mobile computing (employees, contractors, etc.)?
- What are the mobile carrier and pricing options?
- Will carrying devices with enhanced encryption to foreign nations introduce national security risks?
- What is the security risk profile of the proposed mobile device platform?
- What are the communication mechanisms supported by the device? Are there risks associated with them that are unacceptable (e.g., Bluetooth, Wireless Ethernet, Near Field Communication, Infra-Red)?
- Does the mobile device collect data that can be used for purposes other than those directly related to the organization's mission (e.g., location data)?

Applications

- Will the choice of applications that can run on the mobile platform be restricted?
- Will permitted applications include Government, D/A, commercial, and/or open source developed applications?
- Will the application store reside in the cloud or in house?
- Does the organization have the resources to develop applications and services for mobile devices? What framework will the organization follow?
- What testing regimen is required for application updates before they are made available to organization personnel?
- Who will maintain the applications used? If more than one vendor is involved, how are they to communicate when solving problems?
- What software licensing will be required?
- Will the organization require insurance against data breaches (e.g monitoring for lost PII)?
- Will employee application use be monitored during personal-use time?
- Does a vendor maintain control over the application or its data after the application has been deployed (e.g., Amazon Kindle)?
- Does the application collect non-attributable data for use by the vendor in marketing or for other purposes?

Once the organization receives information from several vendors, it can compare the features of the proposed mobile solutions to see which ones best match mission needs, acceptable risk levels, and financial requirements. When a solution is selected, the organization's infrastructure management team (e.g., information security, network operations, and system administrators) and anyone supporting the deployment and implementation of the mobile solution should meet with the vendor to develop an implementation plan. With an agreed-upon implementation plan in hand, procurement can begin.

Not all risks identified in the Risk-Based Tailoring stage will be fully mitigated by an organization's choice of mobile solution infrastructure or policy. Senior management must accept any residual risks; these risks may form the basis of requirements for a future upgrade or modification of the chosen mobile computing solution. If they risks are too great, the organization can revisit the Decision Balancing stage to select a new starting point and use the Risk Based-Tailoring stage to identify a revised set of risks, guidelines, and considerations based on that starting point. The final set of accepted risks is sensitive information because it represents a potential set of vulnerabilities to the mobile computing solution and the organization's business practices. This information should be carefully controlled by the organization.

Conclusion

The Mobile Computing Decision Framework (MCDF) presented in this document is part of a set of deliverables designed to address the Digital Government Strategy (DGS) goals set forth in milestone 9.1. Together, with the other deliverables (e.g., "Mobile Security Reference Architecture," "Mobile Security Baseline,"[15] and "Mobile Device Management IA Controls," the MCDF assists Departments and Agencies in the development of a comprehensive mobile solution strategy to support their missions.

The MCDF's four stages are a roadmap that will help organizations understand how to determine whether a mobile solution is a good fit for their mission, what capability, security, and economic tradeoffs are necessary, and what risks are associated with their mobile solution choices. The results will provide the organization with a high level understanding of the mobile applications, devices, and infrastructure that best fit their needs.

[15] Included in the Mobile Security Baseline is an example of a Federal employee use case for mobile computing and describe in detail application of the MCDF.

Acknowledgments

This document is the product of a multi-agency collaboration to provide guidance for the successful implementation of mobile device solutions for Federal civilian agencies. Participants from several agencies have graciously volunteered their expertise; this document would not be possible without their selfless contributions. Individuals from departments and agencies that contributed to the development of the mobile computing decision framework are as listed below.

Special Acknowledgements

Name	Organization
David Carroll	Department of Homeland Security - Mobile Technology Tiger Team Co-Chair
Kevin Cox	Department of Justice - Mobile Technology Tiger Team Co-Chair
Raj Pillai	General Services Administration - Mobile Technology Tiger Team Co-Chair
Chi Hickey	General Services Administration - Mobile Technology Tiger Team Co-Chair
Joshua Love	White House Communications Agency
Mark Norton	Department of Defense
Greg Youst	Department of Defense
Kelley Dempsey	National Institute for Standards and Technology
Joshua Franklin	National Institute for Standards and Technology
Yonas Ogbaselassie	Department of Homeland Security
Robert Palmer	Department of Homeland Security
Matthew Z. Smith	Department of Homeland Security
Roger Seeholzer	Department of Homeland Security
Kris Lee	Department of Homeland Security
Harry Clarke	National Security Administration

MCDF Document Team

Name	Organization
Marilyn Rose	Department of Homeland Security - Project Manager
Vincent Sritapan	Department of Homeland Security - Project Lead
H. Max Robinson	Department of Homeland Security – Principal Editor
Joel Benge	Department of Homeland Security - Conceptual Designer & Editor

Appendix A

Table 1: NIST SP 800-53 Rev 4 to Risk Mapping

ID	Family	Financial	Policy	Legal	Technical	Operational	Privacy	Security	Total
AC	Access Control		X	X	X		X	X	5
AT	Awareness and Training		X	X	X	X			4
AU	Audit and Accountability		X	X	X		X	X	5
CA	Security Assessment and Authorization		X	X	X	X			4
CM	Configuration Management		X	X	X	X		X	5
CP	Contingency Planning		X	X	X	X			4
IA	Identification and Authentication		X	X	X			X	4
IR	Incident Response		X	X	X	X		X	5
MA	Maintenance	X	X	X	X	X		X	6
MP	Media Protection		X	X	X	X		X	5
PE	Physical and Environmental Protection		X	X	X	X		X	5
PL	Planning		X	X	X	X			4
PS	Personnel Security		X	X	X	X			4
RA	Risk Assessment		X	X	X			X	4
SA	System and Services Acquisition	X	X	X	X	X		X	6
SC	System and Communications Protection		X	X	X		X	X	5
SI	System and Information Integrity		X	X	X	X		X	5
PM	Program Management		X	X	X	X			4
Total		2	18	18	18	13	3	12	